

TOM DAVIS, VIRGINIA,
CHAIRMAN

DAN BURTON, INDIANA
CHRISTOPHER SHAYS, CONNECTICUT
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. McHUGH, NEW YORK
JOHN I. MICA, FLORIDA
MARK E. SOUDER, INDIANA
STEVEN C. LATOURETTE, OHIO
DOUG OSE, CALIFORNIA
RON LEWIS, KENTUCKY
JO ANN DAVIS, VIRGINIA
TODD RUSSELL PLATTIS, PENNSYLVANIA
CHRIS CANNON, UTAH
ADAM H. PUTNAM, FLORIDA
EDWARD L. SCHROCK, VIRGINIA
JOHN J. DUNCAN, JR., TENNESSEE
JOHN SULLIVAN, OKLAHOMA
NATHAN DEAL, GEORGIA
CANDICE MILLER, MICHIGAN
TIM MURPHY, PENNSYLVANIA
MICHAEL R. TURNER, OHIO
JOHN R. CARTER, TEXAS
WILLIAM J. JANKLOW, SOUTH DAKOTA
MARSHA BLACKBURN, TENNESSEE

ONE HUNDRED EIGHTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074
FACSIMILE (202) 225-3974
MINORITY (202) 225-5051
TTY (202) 225-6852

www.house.gov/reform

HENRY A. WAXMAN, CALIFORNIA,
RANKING MINORITY MEMBER

TOM LANTOS, CALIFORNIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
CAROLYN B. MALONEY, NEW YORK
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
WM. LACY CLAY, MISSOURI
DIANE E. WATSON, CALIFORNIA
STEPHEN F. LYNCH, MASSACHUSETTS
CHRIS VAN HOLLEN, MARYLAND
LINDA T. SANCHEZ, CALIFORNIA
C. A. DUTCH RUPPERSBERGER,
MARYLAND
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
JIM COOPER, TENNESSEE
CHRIS BELL, TEXAS

BERNARD SANDERS, VERMONT,
INDEPENDENT

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

Oversight Hearing

“Cyber Security: The Status of Federal Information Security and the Effects of the Federal Information Security Management Act at Federal Agencies.”

Tuesday, June 24, 2003

Opening Statement

Chairman Adam Putnam (R-FL)

Good morning. A quorum being present, this hearing of the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census will come to order. Good morning and welcome to the second in a planned series of hearings addressing the important subject of cyber security.

Today we continue our in-depth review of cyber security issues affecting our nation. Specifically this hearing will focus sharply on the efforts within the Federal Government to secure our own computer networks. Our critical infrastructure, of the cyber kind, must have the same level of protection as our physical security, if we are to be secure, as a Nation, from random hacker intrusions, malicious viruses or worse – serious cyber terrorism.

There are several things unique to cyber attacks that make the task of preventing them particularly difficult. Cyber attacks can occur from anywhere around the globe: from the caves of Afghanistan to the war fields of Iraq, from the most remote regions of the world or simply right here in our own back yard. The technology used for cyber attacks is readily available and changes continually. And, maybe most dangerous of all, is the failure of many people -- critical to securing these networks and information from attack -- to take the threat seriously, to receive adequate training, and to take steps needed to secure their networks. A serious cyber attack could have serious repercussions throughout the nation both in a physical sense and in very real economic dollars.

A recent report under Government Information Security Reform Act (GISRA) once again demonstrates that we have a long way to go in the Federal government to feel the least bit confident that we have secure computer networks. Before going into more detail about the report, I want to comment briefly about the timing. This latest GISRA report was released this May. It was based on information provided to OMB in September of 2002! This is kind of like being an astronomer and looking into a telescope at the stars all the while realizing that what you are viewing happened a long long time ago. We need to find a way to get more real time reporting and I want to work with OMB on that aspect of the reporting.

The current GISRA Report demonstrates that progress in computer security at Federal agencies is proceeding slowly and that simply is no longer acceptable. The OMB report to Congress identified a number of serious weaknesses:

- Many agencies are facing the same security weaknesses year after year, such as lack of system level security plans and certifications and accreditations;
- Some IGs and CIOs -- from within the same agencies -- have vastly different views of the state of the agency's security programs;
- Many agencies are not adequately prioritizing their IT investments and are seeking funding to develop new systems while significant weaknesses exist in their legacy systems;
- Not all agencies are reviewing all programs and systems every year as required by GISRA;
- More agency program officials must engage and be held accountable for ensuring that the systems that support their programs and operations are secure. The old thinking of IT security as the responsibility of a single agency official or the agency's IT security office is out of date, contrary to law and policy, and significantly endangers the ability of agencies to safeguard their IT investments.

The Departments of Treasury, State and Agriculture all have serious problems with their information security. Both the CIOs and the IGs of these agencies have concerns. In addition, GAO has indicated a concern with computer security for all three agencies in its Performance and Accountability Series.

In the FY 2002 GISRA report, the Department of Agriculture reported that less than 26% of its systems were in compliance with the 8 metrics that OMB reported. The agency had 70 material weaknesses in the area of information security reported by the IG.

In addition, according to the IG, the agency is not conducting risk assessments of its systems in compliance with either OMB or GISRA requirements. This year, the agency reported an increase in systems operating without written authority, and an increase in systems that do not have up-to-date IT security plans.

The Department of State did not report information for the FY 2001 GISRA report. It reported 3 material weaknesses for information security for FY 2002. In June 2001, the Department's IG released a report that highlighted a number of areas that State needs to address.

These areas included assessing vulnerability of systems, conducting security control evaluations at least once every three years, and testing security controls. State reported, in the FY 2002 GISRA report, that none of its systems have been certified and authorized, and only 15% have an up-to-date IT security plan. Finally, State reported that only 11% of its systems have contingency plans, and of those, none had ever been tested.

Although the Department of Treasury reported that in the FY 2002 GISRA report that 41% of its systems were assessed for risk, its IG reported that Treasury did not use an adequate methodology to determine risk. Therefore, its assessments were not valid under GISRA.

There are also significant discrepancies in many of the metrics reported in the GISRA report between the Department and its IG. For example, the Department reported that 451 of its systems were reviewed. However, the IG reports that only 204 systems were reviewed. Treasury has also reported 11 material weaknesses related to information security.

I understand that many of those testifying today are relatively new to their jobs. We're not here, today, to point fingers, although I have serious questions about accountability and responsibility for these egregious failures to perform minimum requirements, we are here to identify weaknesses or roadblocks, find solutions and make progress.

In a recent edition of the *Federal Times* headlined "Computer Security Dilemma: Agencies Must Choose – Follow the Law or Fix the Problem," several government IT managers complain that the documentation process set up by Congress gives them a choice: document their security problems for Congress or fix them.

To say that I am disturbed by this attitude would be an understatement. For most IT managers the documentation process set up by Congress is the only reason they discovered many of their security weaknesses. Before the documentation process, many IT managers couldn't even identify their critical systems.

Sadly, even with the documentation process required by Congress, many systems are still unidentified. All that being said, I will try and remain open minded and if any of the witnesses today would like to support this either/or contention I would like to hear it.

As the subcommittee continues to examine the cyber security issue, we see the same recurring theme. Securing these networks is not about money or technology but about people and management. The weaknesses identified are weaknesses that would be significantly reduced if approved procedures and protocols or best practices were actually followed.

For example GAO still conducts audits to this day where they find default passwords in place or where systems have not been tested in a production environment. Patches remain uninstalled on systems for months after known vulnerabilities are identified. These rudimentary lapses are simply not acceptable.

There are a number of issues still up for consideration for the Congress. These include:

- Requiring that the Common Criteria be the standard government-wide.

- Automated vulnerability scanning.
- New levels of accountability.
- Confronting the issue of CIO retention head-on.

While some progress is clearly being made at federal agencies, going from an F to a D or D to a C isn't saying much. It's my hope that the Congress, OMB, the CIOs, the IGs and the GAO can work together to move our level of IT security government-wide into a range where we have some relative degree of comfort that our systems are secure. We are a long way from that point today.

I would like to thank all the witnesses for coming today and presenting your valuable testimony.